The CIO Guide to API Security: Enabling Innovation Without Enabling Attacks and Data Breaches

Mark O'Neill
15 November 2018

Gartner®

By 2022, API abuses will be the most frequent attack vector resulting in data breaches for enterprise web applications.

Source: "How to Build an Effective API Security Strategy" (G00342236)

Gartner

API Security

1. What exactly are the security problems with APIs?
2. What can be done about API security?
3. Where should you start?

Gartner

API Security

1. What exactly are the security problems with APIs?
2. What can be done about API security?
3. Where should you start?

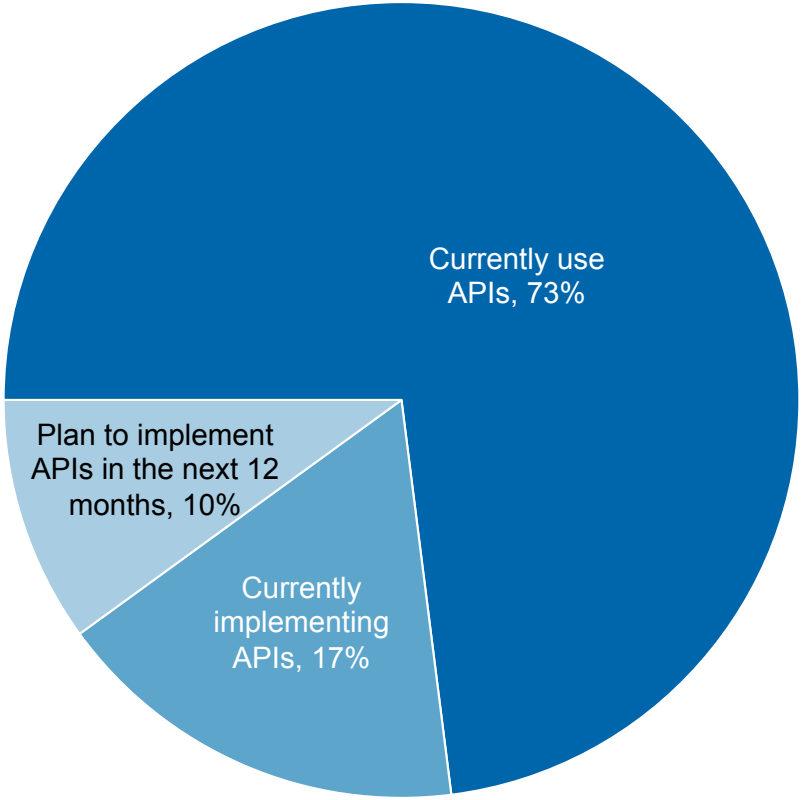
Gartner

APIs Are Intended to Be Easy to Use

- Commonly understood technologies:
  - JSON, web protocols, XML
- Typically published in a developer portal:
  - … or used “under the hood” in a web or mobile framework
- Emphasis is placed on “Quick time to Hello World”

Gartner

Most organizations currently use APIs



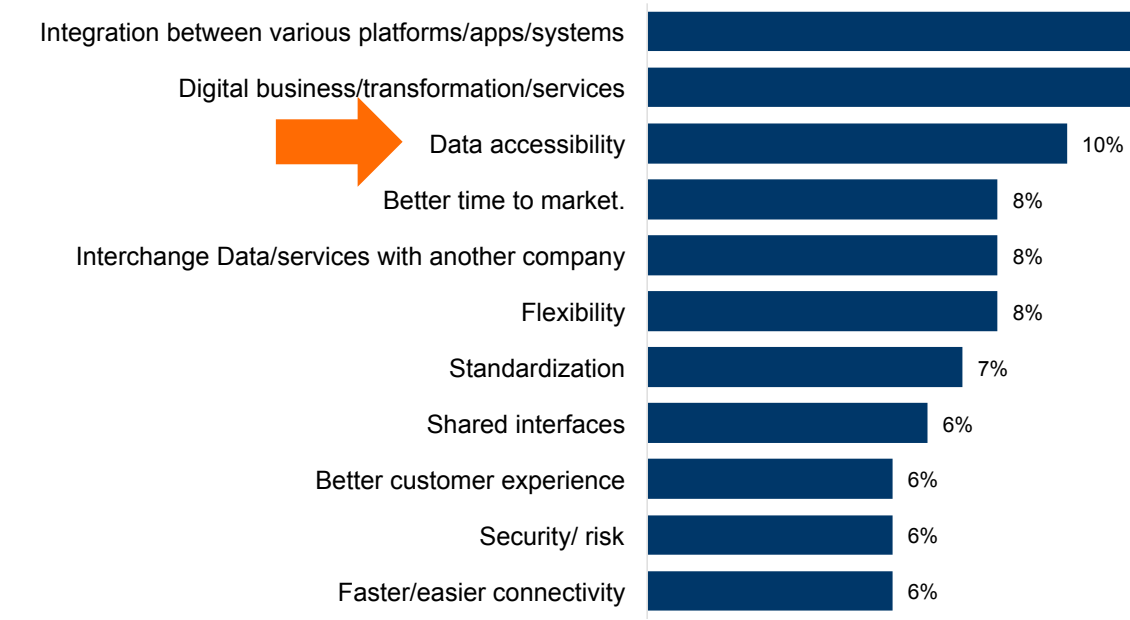
Source: Gartner Survey “API Usage and its Role in Digital Platform Growth Report” 2018

Gartner

APIs are often implemented to help with integration and data access but also digital business

Top business goals or objectives organizations address with APIs (coded)

Percent of respondents



Other mentions

Data flow	4%
Improve business processes	4%
Reusability	4%
Automation	3%
Cost efficiencies	3%
Innovation	3%
Interchange Data/services with customer	3%
Legacy modernization	2%
New/ improved services/products	2%
Regulation (PSD2)	2%
Mobile applications	2%
Decoupling customer engagement systems	2%
Easier application assembly	2%
Increase revenue	2%
Platform strategy	2%
User experience	2%
Data monetization	1%
Other	2%

Gartner

APIs are often implemented to help with integration and data access

Business goal or objective organizations address with APIs (open-ended)

APIs gives business **more agility** in their project, gives them the ability to **get more value from the information** that are no longer hidden in an application, but exposed with APIs.

Improve **integration** between new and legacy applications. **Standardize** how business functionality exposed by APIs is **governed, managed and consumed**.

Re-usable integration platform in support of a **common information model**. Ability to increase the reuse of integration points. Ability to incorporate business rules within the API transactions for data/record validation.

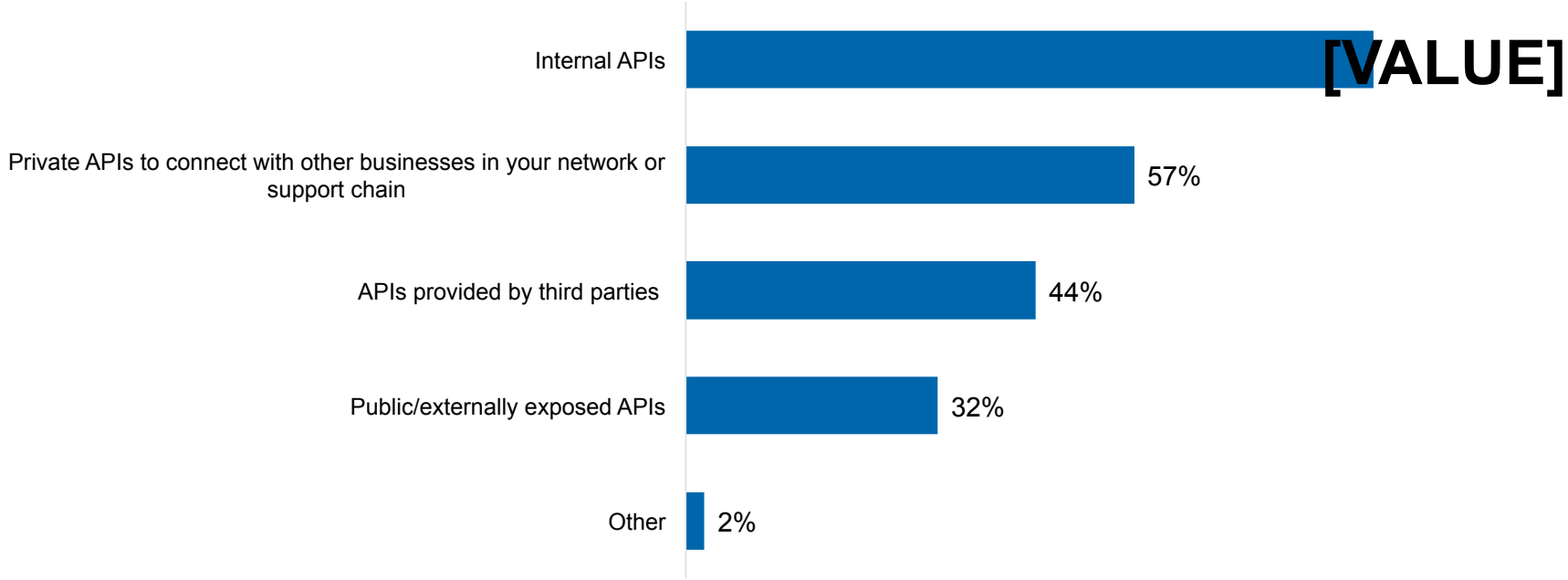
Standardize processes for data access across teams and reuse where possible, manage through governance, monitor and manage response.

Gartner

Internal APIs are widespread; less than a third plan to deploy public / externally exposed APIs

Types of API's organizations currently use/plan to use

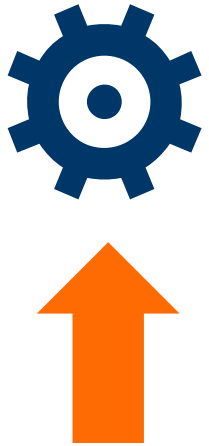
Percent of respondents



Gartner

Attackers Go After Targets That Are the Most Valuable

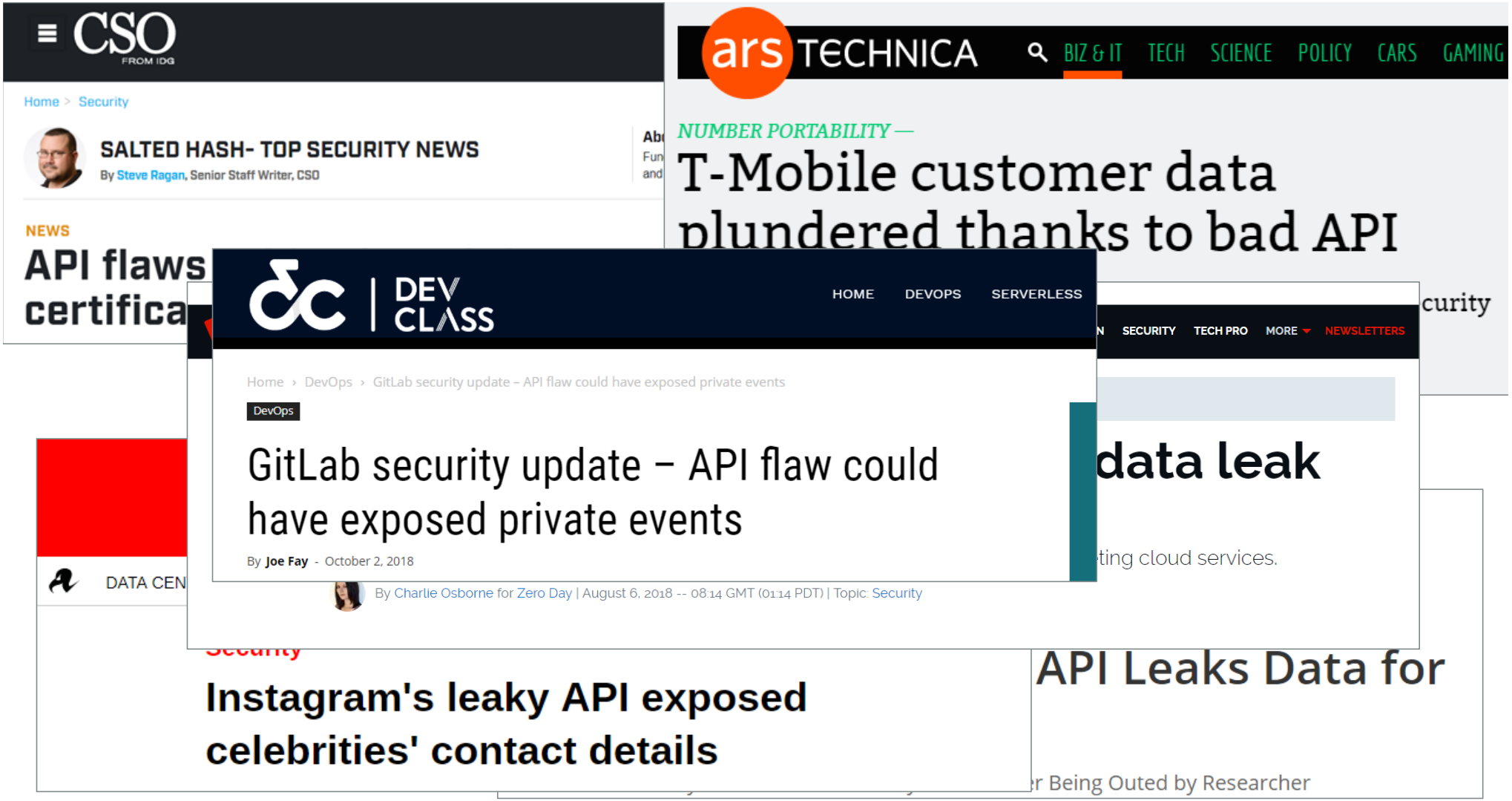
Calls APIs



- Data breaches
- Denial of Service
- “Scraping” attacks

The data and applications are here

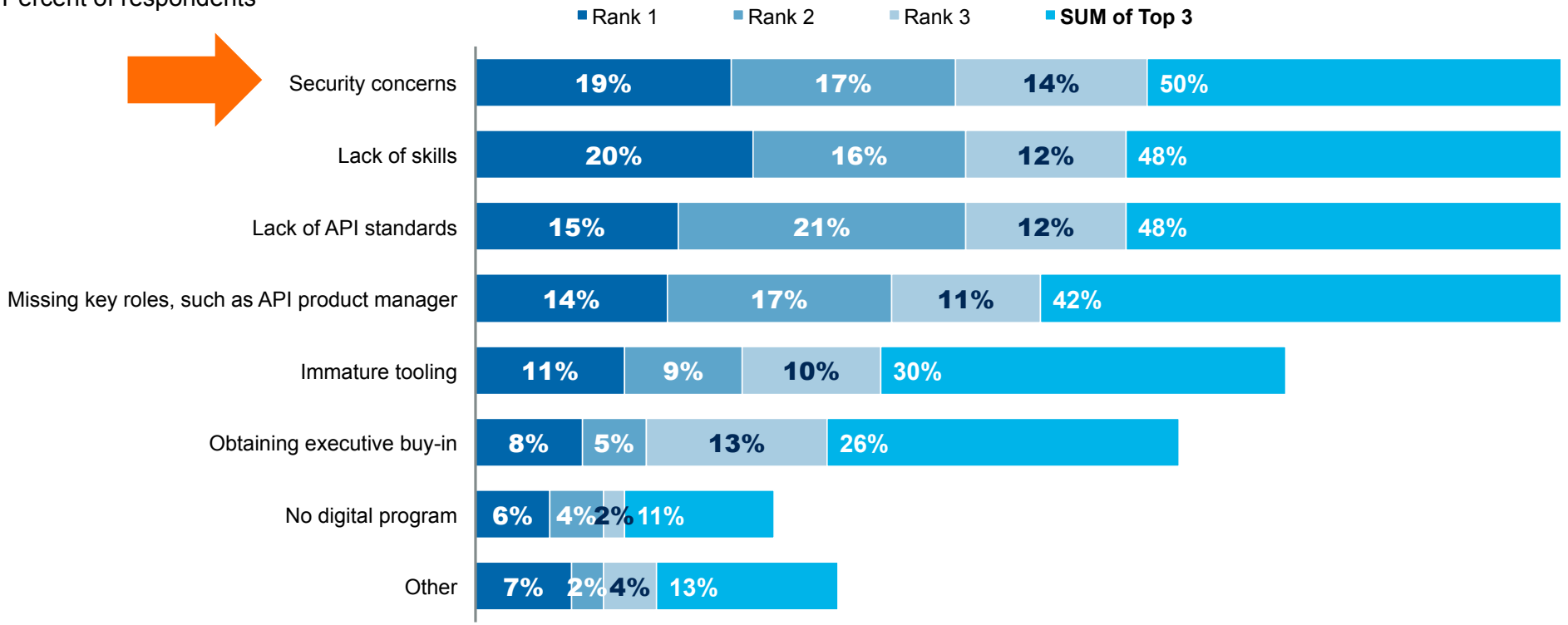
Gartner


CSO
FROM IDG
Home > Security
SALTED HASH- TOP SECURITY NEWS
By Steve Ragan, Senior Staff Writer, CSO
NEWS
API flaws
certifica
ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING
NUMBER PORTABILITY —
T-Mobile customer data plundered thanks to bad API
curity
DEV CLASS
HOME
DEVOPS
SERVERLESS
SECURITY
TECH PRO
MORE
NEWSLETTERS
Home › DevOps › GitLab security update – API flaw could have exposed private events
DevOps
GitLab security update – API flaw could have exposed private events
By Joe Fay - October 2, 2018
data leak
ting cloud services.
DATA CEN
By Charlie Osborne for Zero Day | August 6, 2018 -- 08:14 GMT (01:14 PDT) | Topic: Security
Instagram's leaky API exposed celebrities' contact details
API Leaks Data for
r Being Outed by Researcher

Good News: There Is Awareness of the Problem

Gartner Research Circle

The top 3 challenges to organizational API strategy
Percent of respondents



Gartner

API Security

1. What exactly are the security problems with APIs?
2. What can be done about API security?
3. Where should you start?

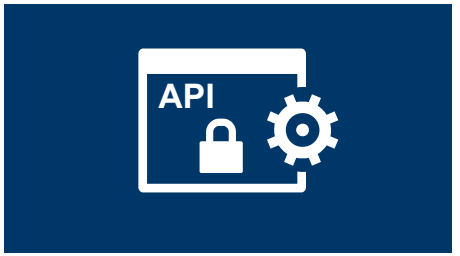
Gartner

Follow These Three Steps

1. **Discover:** Inventory APIs that have been delivered, or are in the development process. APIs consumed from third-parties should also be included.

2. **Monitor:** Observe your API usage. Learn what “normal” is for API behavior.

3. **Secure:** Create a policy to secure your APIs.



Gartner

Designing an API Management and Security Policy

- Think about:
  - How your APIs will be used (Mobile clients? Application-to-application traffic?)
  - Expected API usage patterns
  - Internal vs. external usage
  - Where API gateways can be placed (Cloud/On-premises/Both?)
  - Potential threats to your APIs
  - Authentication of both end users and API clients
  - Data security

Gartner

Web Application Firewalls (WAFs) and API Gateways

WAF: Threat Protection

- DDoS protection
- Bot mitigation
- Attack signatures (OWASP)
- Whitelist management
- Anomaly detection

API Gateway: API Access Control

- Transformation/Orchestration
- Per-API authorization management
- Performance optimization (caching)
- Scope management — throttling

API gateway is the application delivery controller for APIs.
WAFs provide threat detection for public-facing web applications.

Gartner

API Security

1. What exactly are the security problems with APIs?
2. What can be done about API security?
3. **Where should you start?**

Gartner

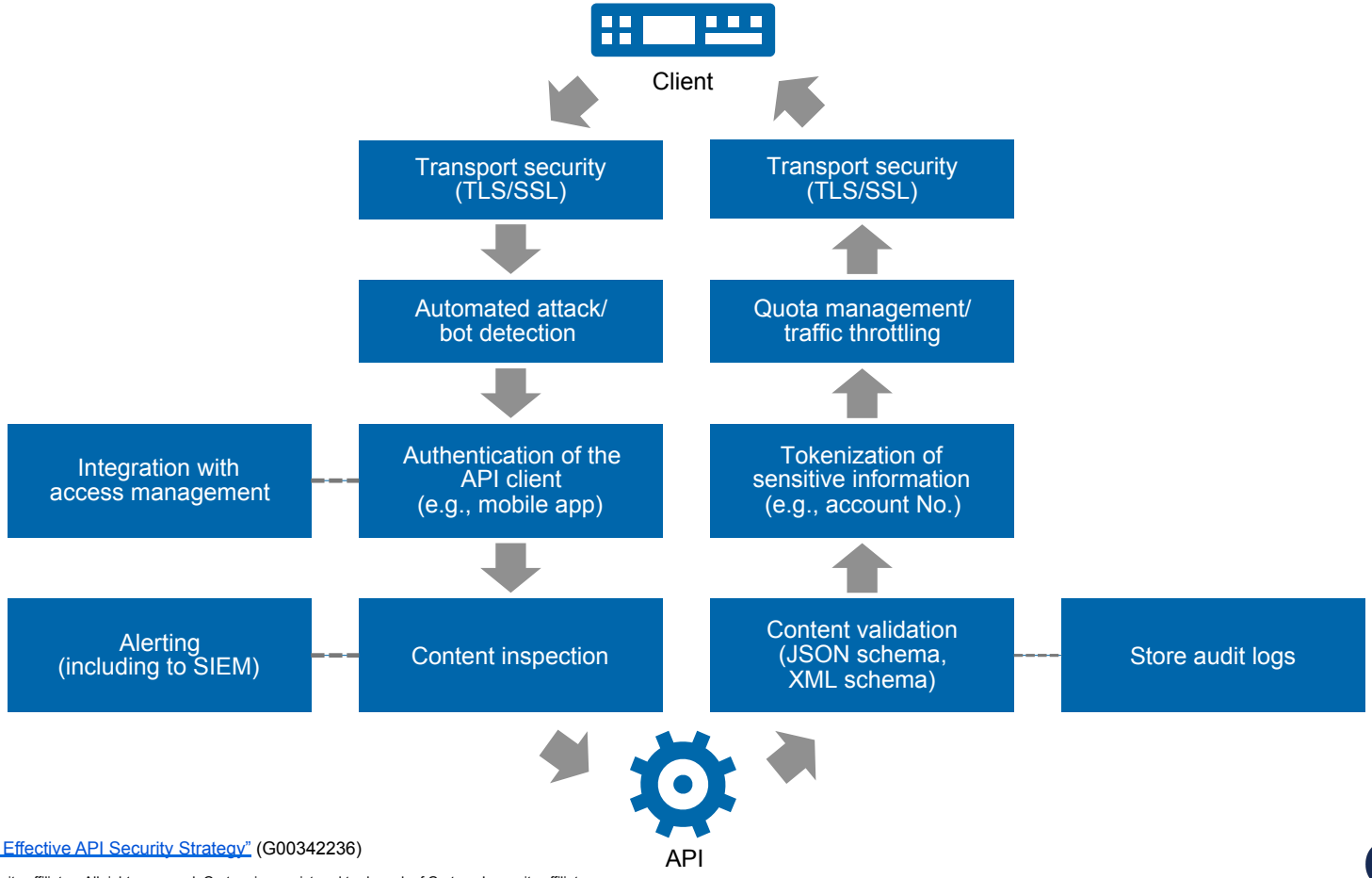
Your API Security Building Blocks

Authentication of the API client (e.g., mobile app)	Authentication of the end user	Quota management/ traffic throttling
Content inspection	Content validation (JSON schema, XML schema)	Tokenization of sensitive information (e.g., account No.)
Automated attack/ bot detection	Transport security (TLS/SSL)	Content encryption/ decryption
Store audit logs	Signature validation	API key management
Token Issuance (OAuth 2.0, JWT Token)	Fine-grained authorization (e.g., on OAuth scopes)	Third-party identity provider (IdP) or social login
Integration with access management	XML/SOAP security (WS-security, etc.)	Alerting, including to security incident event management (SIEM)

Source: "How to Build an Effective API Security Strategy" (G00342236)

Gartner

Creating an Effective API Security Policy



Source: "How to Build an Effective API Security Strategy" (G00342236)

Gartner

Recommendations

- ✓ Start and maintain an inventory of your APIs:
  - Discover the APIs you have built
  - Also inventory the APIs you consume from others
- ✓ Construct API security policies that include:
  - Authentication and authorization
  - Attack protection
  - Data security

Gartner

Recommended Gartner Research

- **How to Build an Effective API Security Strategy**
  Mark O'Neill, Dionisio Zumerle and Jeremy D'Hoinne (G00342236)
- **Selecting the Right API Gateway to Protect Your APIs and Microservices**
  Mary Ruddy and Michael Isbitski (G00349440)
- **Managing the Consumption of Third-Party APIs**
  Mark O'Neill (G00348312)
- **Magic Quadrant for Full Life Cycle API Management**
  Paolo Malinverno and Mark O'Neill (G00319327)
- **Critical Capabilities for Full Life Cycle API Management**
  Mark O'Neill and Paolo Malinverno (G00334223)

Gartner